

REMARKS/ARGUMENTS

Prior to the entry of this Amendment, claims 1-9, 11-37, and 40-42 were pending in this application. Claims 1 and 41 have been amended herein. No claims have been added and claims 20-32 and 35-37 have been canceled. Therefore claims 1-9, 11-19, 33-34, and 40-42 remain pending in the application. Applicants respectfully request reconsideration of this application for at least the reasons presented below.

35 U.S.C. §103 Rejection, Colligan in view of Wasilewski

The Office Action has rejected claims 1-2 and 41-42 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,415,031 of Colligan et al. (hereinafter "Colligan") in view of U.S. Patent No. 6,516,412 of Wasilewski et al. (hereinafter "Wasilewski"). The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

In order to establish a *prima facie* case of obviousness, the Office Action must establish: 1) some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine their teachings; 2) a reasonable expectation of success of such a modification or combination; and 3) a teaching or suggestion in the cited prior art of each claimed limitation. See MPEP §706.02(j). As will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation.

Colligan "relates to secure video distribution networks" (col. 1, lines 23-24) and teaches "selective and renewable encryption for secure distribution of digital video on-demand" (col. 1, line 67 - col. 2, line 1). Under Colligan, "renewable encryption is provided in a process which includes: copying a first encrypted digital video program from a remote server to a video

Amdt. dated: January 4, 2006
Reply to Office Action of October 5, 2005

source; decrypting the first encrypted digital video program using a first key to generate an unencrypted digital video program; encrypting the unencrypted digital video program using a second key to generate a second encrypted digital video program; transmitting the second encrypted digital video program from the video source to the remote server; and deleting the first encrypted digital video program from the remote server." (Col. 2, lines 11-20) That is, Colligan teaches performing a renewal process at the end of a "time epoch." (Col. 8, lines 41-57) Under this periodic renewal process, a copy of the original encrypted content is decrypted with the first key, re-encrypted with a second, new key, the re-encrypted content is made available for distribution, and the original encrypted content is deleted. (Col. 8, line 58 - col. 9, line 17)

However, as pointed out on page 3 of the Office Action, Colligan does not teach or suggest "an encryption renewal system generating time limited entitlement control messages (ECMs) allowing the pre-encrypted content to be decryptable for a time limited designated duration." Furthermore, Colligan does not teach or suggest periodic entitlement control message renewal without re-encrypting the pre-encrypted content. Rather, Colligan teaches a renewal process in which the content is decrypted and re-encrypted with a new key.

Wasilewski relates to "protecting information that is transmitted by means of a wired or wireless medium against unauthorized access." (Col. 1, lines 45-47) Under Wasilewski, "when the service distribution organization broadcasts an instance of the service, it encrypts or scrambles the instance to form [an] encrypted instance." (Col. 4, lines 26-29) That is, Wasilewski teaches real-time encryption or encryption as the content is being broadcast. The real-time encryption of Wasilewski includes using a control word (CW) to encrypt the content. (Col. 6, lines 25-38) The CW is in turn encrypted with a Multi-Session Key (MSK) and included in an ECM. (Col. 6, lines 40-45) The CW used to encrypted the content and the MSK used to encrypt the CW can be periodically changed and distributed. (Col. 6, lines 38-56)

However, Wasilewski does not teach or suggest generating time limited entitlement control messages (ECMs) allowing the pre-encrypted content to be decryptable for a

Amdt. dated: January 4, 2006
Reply to Office Action of October 5, 2005

time limited designated duration. Rather the CW and MSK of Wasilewski are periodically changed similar to Colligan's teaching of periodically replacing the encryption key. Additionally, Wasilewski does not teach or suggest pre-encrypting content. Rather, Wasilewski teaches real-time encryption of content as is being broadcast. Furthermore, Wasilewski's reliance on real-time encryption and Colligan's stated reasons for not using real-time encryption (col. 1, lines 52-59), would seem to negate any motivation to combine the references.

Claim 1, upon which claim 2 depends, and claim 41, upon which claim 42 depends, both recite in part "a content preparation module for pre-encrypting the content offline to form pre-encrypted content; . . . an encryption renewal system . . . to generate time limited entitlement control messages allowing the pre-encrypted content to be decryptable for a time limited designated duration; . . . wherein said encryption renewal system performs periodic entitlement control message renewal . . . without re-encrypting the pre-encrypted content." Neither Colligan nor Wasilewski, alone or in combination, teach or suggest generating time limited entitlement control messages (ECMs) allowing the pre-encrypted content to be decryptable for a time limited designated duration or periodic entitlement control message renewal without re-encrypting the pre-encrypted content.. Rather, Colligan teaches a renewal process in which the content is decrypted and re-encrypted with a new key while Wasilewski teaches a real-time encryption process in which the keys are periodically changed. For at least these reasons, claims 1, 2, 41, and 42 should be allowed.

35 U.S.C. §103 Rejection, Bertram in view of Wasilewski

The Office Action has rejected claims 3, 5-14, and 17-19 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0140340 of Bertram (hereinafter "Bertram") in view of Wasilewski. The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Specifically, as will be discussed in detail below, the references cited by the Office Action do not

teach or suggest each claimed limitation. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As described above, Wasilewski fails to teach or suggest pre-encrypting content prior to receiving a request for the content. Furthermore, Wasilewski fails to teach or suggest generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. Rather, Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed.

Bertram "relates to a method and apparatus for applying conditional access impulse authorization techniques to information on demand services such as video on demand services." (para. 3) Under Bertram, a content stream is encrypted (para. 45) and descrambling messages and impulse authorizations are embedded into the encrypted content stream (para 46). "The impulse authorization is a conditional access message usable by any set top terminal to allow that set top terminal to use a descrambling key to descramble a particular content stream." (para. 47) However, Bertram fails to disclose any way in which the impulse authorization or descrambling messages may be updated. Therefore, as the Office Action states on pages 4 and 5, Bertram does not teach or suggest "generating time limited control messages for permitting access to the pre-encrypted content." Furthermore, Bertram does not teach or suggest periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires.

Claim 3, upon which claims 5-9 and 11-14 depend, recites in part "pre-encrypting, . . . the content to form pre-encrypted content . . . generating one or more time limited control messages for permitting access to the pre-encrypted content; . . . and periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires." Neither reference,

Amdt. dated: January 4, 2006
Reply to Office Action of October 5, 2005

alone or in combination, teaches or suggests generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. Rather, Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed while Bertram fails to disclose any way in which the impulse authorization or descrambling messages may be updated. For at least these reasons, claims 3, 5-9, and 11-14 should be allowed.

Claim 17, upon which claims 18 and 19 depend, recites in part "means for pre-encrypting the first and second content offline to form first and second pre-encrypted content . . . means for generating a first and second time limited entitlement messages that allow decryption of the first and second pre-encrypted contents, respectively; . . . wherein said means for generating said first and said second time limited entitlement messages performs periodic entitlement control message renewal." Neither reference, alone or in combination, teaches or suggests generating time limited entitlement messages that allow decryption of the pre-encrypted contents or performing periodic entitlement control message renewal. Rather, Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed while Bertram fails to disclose any way in which the impulse authorization or descrambling messages may be updated. For at least these reasons, claims 17-19 should be allowed.

35 U.S.C. §103 Rejection, Bertram and Wasilewski in view of Dunn

The Office Action has rejected claims 4, and 15-16 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of Wasilewski and further in view of U.S. Patent No. 6,154,772 of Dunn et al. (hereinafter "Dunn"). The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Specifically, as will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As described above, Bertram and Wasilewski, alone or in combination, fail to teach or suggest generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. Rather, Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed while Bertram fails to disclose any way in which the impulse authorization or descrambling messages may be updated.

Dunn "the delivery of digital video and data over a communication channel." (Col. 1, lines 27-28) Under the method of Dunn, "a plurality of video channels are simultaneously placed on a bus; a request from a user for at least one of the plurality of video channels is received; the request is processed in order to determine whether the user is authorized to receive at least one of the plurality of video channels; and at least one of the plurality of video channels is delivered over a communications channel to the user if the user is authorized to receive the at least one of the plurality of video channels." (Col. 2, line 61 - col. 3, line 6) However, Dunn makes no mention of encrypting the content, either pre-encrypting or in real-time. Rather, content is sent to a user if the user is authorized based on a centralized table of authorization information. (Col. 6, lines 37-50)

Claim 3, upon which claims 4, and 15-16 depend, recites in part "pre-encrypting, . . . the content to form pre-encrypted content . . . generating one or more time limited control messages for permitting access to the pre-encrypted content; . . . and periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires." None of the references, alone or in combination, teach or suggest generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. Rather, Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed while Bertram

fails to disclose any way in which the impulse authorization or descrambling messages may be updated. Under Dunn, content is sent to a user if the user is authorized based on a centralized table of authorization information. For at least these reasons, claims 4, 15 and 16 should be allowed.

35 U.S.C. §103 Rejection, Bertram and Wasilewski in view of Colligan

The Office Action has rejected claims 33 and 34 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of Wasilewski and further in view of Colligan. The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Specifically, as will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As described above, Bertram, Wasilewski, and Colligan, alone in combination, fail to teach or suggest generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. Rather, Bertram teaches applying conditional access impulse authorization techniques to information on demand services but fails to disclose any way in which the impulse authorization or descrambling messages may be updated. Wasilewski teaches a real-time encryption process in which the keys are periodically changed and distributed. Colligan teaches a renewal process in which the content is decrypted and re-encrypted with a new key.

Claim 3, upon which claims 33 and 34 depend, recites in part "pre-encrypting, . . . the content to form pre-encrypted content . . . generating one or more time limited control messages for permitting access to the pre-encrypted content; . . . and periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting

access to the pre-encrypted content after the first key information expires." None of the references, alone or in combination, teach or suggest generating one or more time limited control messages for permitting access to the content or periodically retrofitting a second time limited entitlement control message to the pre-encrypted content for permitting access to the pre-encrypted content after the first key information expires. For at least these reasons, claims 33 and 34 should be allowed.

35 U.S.C. §103 Rejection, Bertram in view of Candelore

The Office Action has rejected claims 20, 22-24, and 26-31 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of U.S. Patent No. 6,363,149 of Candelore (hereinafter "Candelore"). As claims 20, 22-24, and 26-31 have been cancelled, the Applicants submit that this rejection has been rendered moot.

35 U.S.C. §103 Rejection, Bertam and Candelore in view of Dunn

The Office Action has rejected claims 21 and 32 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of Candelore and further in view of Dunn. As claims 21 and 32 have been cancelled, the Applicants submit that this rejection has been rendered moot.

35 U.S.C. §103 Rejection, Bertam and Candelore in view of Colligan

The Office Action has rejected claims 25 and 35-37 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of Candelore and further in view of Colligan. As claims 25 and 35-37 have been cancelled, the Applicants submit that this rejection has been rendered moot.

Appl. No. 09/898,184
Amdt. dated: January 4, 2006
Reply to Office Action of October 5, 2005

PATENT

35 U.S.C. §103 Rejection, Bertram and Candelore in view of Safadi

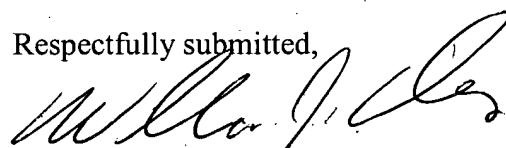
The Office Action has rejected claim 40 under 35 U.S.C. §103(a) as being unpatentable over Bertram in view of Candelore and further in view of U.S. Patent No. 6,256,393 of Safadi et al. (hereinafter "Safadi"). As claim 40 has been cancelled, the Applicants submit that this rejection has been rendered moot.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,



William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 303-571-4321

WJD/sbm
60669836 v1